ZK LOWER BOUNDS and LIMITATIONS

ALON ROSEN

IDC HERZLIYA

FOUNDATIONS & APPLICATIONS of CRYPTOGRAPHIC THEORY

The Goal

<u>Goal</u>: understand the limitations of ZK

- The role of interaction
- The role of randomness
- Black-Box simulation
- Public-coin vs private coin
- Parallel/concurrent composition

Deterministic/ non-interactive ZK

Recall: a proof that is <u>not</u> ZK

$x \in QR_N$: $\xrightarrow{\pi = w}$ **V** $x \stackrel{?}{\equiv} w^2 \, mod \, N$

- **Proof is non-interactive**
- V **is deterministic**
- P **is deterministic**

Can we build "error-free" ZK **for** $L \notin \mathrm{BPP}$**?**

<u>**Note**</u>: ZK **for** $L \in \mathrm{BPP}$ **is considered "trivial"**

Triviality of error-free ZK

- **Unidirectional proof**: a single message from P to V
- **Example**: NP proofs

Theorem: Suppose that L has a unidirectional ZK proof. Then $L \in \mathrm{BPP}$

Theorem: Suppose that L has a ZK proof in which the verifier V is deterministic. Then $L \in \mathrm{BPP}$

Theorem: Suppose that L has an auxiliary-input ZK proof in which the prover P is deterministic. Then $L \in \mathrm{BPP}$

Triviality of unidirectional ZK

Theorem: Suppose that L has a unidirectional ZK proof. Then $L \in \mathrm{BPP}$

- Let $(w, r) = S(x)$ be the simulator's output on input x
- To decide L, pick random independent s and run $V(w, s)$

Claim: If $x \in L$ then $Pr_s[V(w, s) = \text{ ACCEPT}] \geq 2/3$

Otherwise, can distinguish $S(x) = (w, r)$ from $(P, V)(x)$

Claim: If $x \notin L$ then $Pr_s[V(w, s) = \text{ ACCEPT}] \leq 1/3$

Otherwise, P^* that sends simulator's w violates soundness

Triviality of ZK with deterministic V

<u>Theorem</u>: Suppose that L has a ZK proof in which the verifier V is deterministic. Then $L \in \mathrm{BPP}$

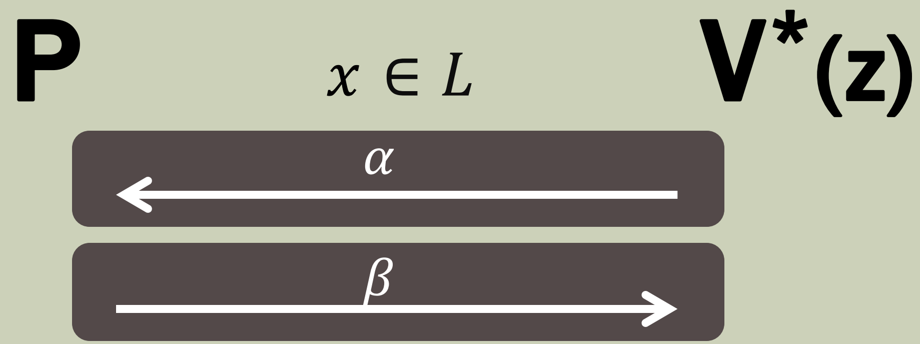
- If V is deterministic then P can fully determine all of V's future messages
- So P can precompute the transcript and send it over to V
- The new proof system inherits completeness, soundness and zero-knowledge properties from the original proof
- The new proof system is unidirectional and so $L \in BPP$

<u>Theorem</u>: Suppose that L has an auxiliary-input ZK proof in which the prover P is deterministic. Then $L \in \mathrm{BPP}$

Triviality of 2-round ZK

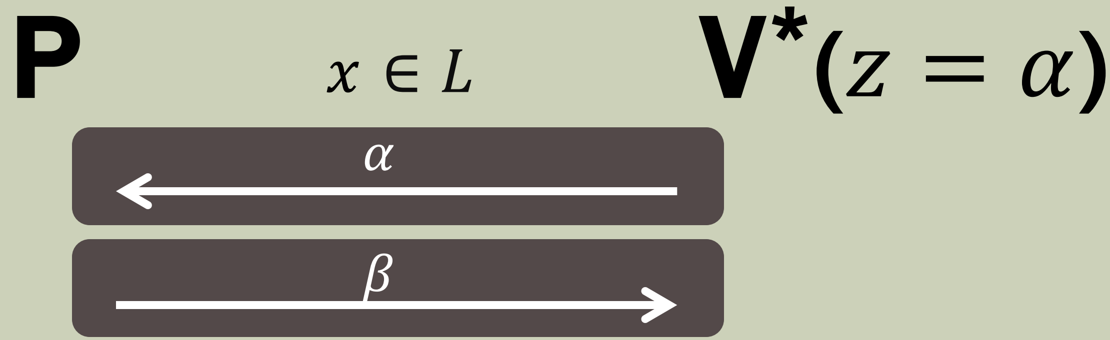
Theorem: Suppose that L has a 2-round auxiliary-input ZK proof. Then $L \in \mathrm{BPP}$

- **Recall: 2-round proof for $\overline{QR_N}$ is not auxiliary-input ZK**
- **[BLV'02]: even without aux input (complexity assumptions)**



- **Let $S(x)$ be the simulator's output on input x**
- **Consider a verifier $V^*(x, z = \alpha)$ that on auxiliary input z sends $z = \alpha$ as its first message**

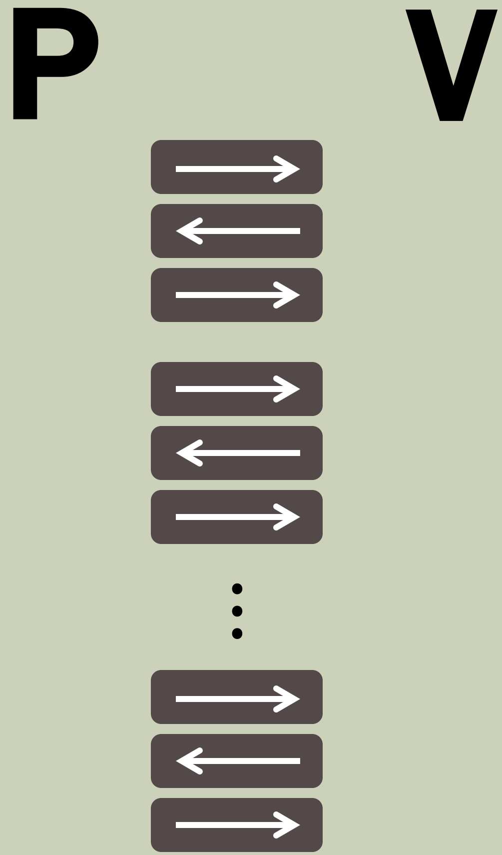
Triviality of 2-round ZK



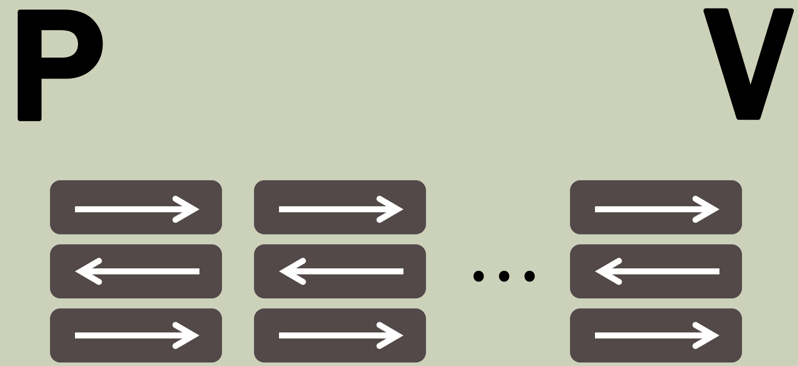
- To decide if $x \in L$
  - pick random r and compute $\alpha = V(x, r)$
  - Run $S(x, \alpha)$ with $V^*(x, \alpha)$ and accept if and only if S outputs an accepting view for V^*
- <u>Note</u>: all we did is substitute the simulator for the prover as a means of generating β
- $x \in L$ is accepted because of completeness of (P, V)
- $x \notin L$ is rejected because of soundness of (P, V)

Black-Box ZK

Sequential vs Parallel Repetition

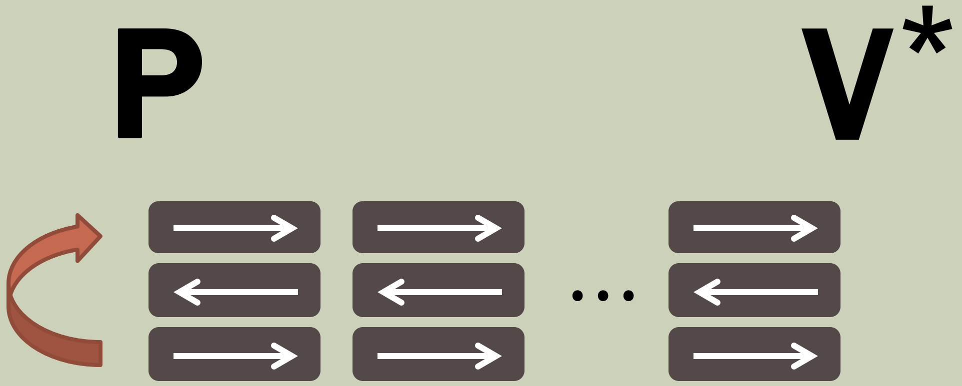


- **Negligible soundness**
- **High round complexity**
- ZK



- **Negligible soundness**
- **Low round complexity**
- ZK**?**

Constant-round ZK for NP



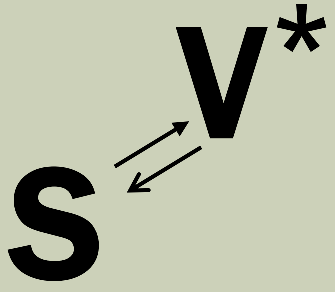
- Problem: V^*'s challenge is a string $\boldsymbol{b} \in_R \{0,1\}^k$
- Simulator's expected number of guessing attempts is 2^k
- Solution: Let verifier commit to $\boldsymbol{b}$ in advance

- Yields 5 round proof (assuming OWF, 4-round argument)
- Question: can V be public-coin?
- Question: do 3-round protocols exist?

Public-coin and Black-Box ZK

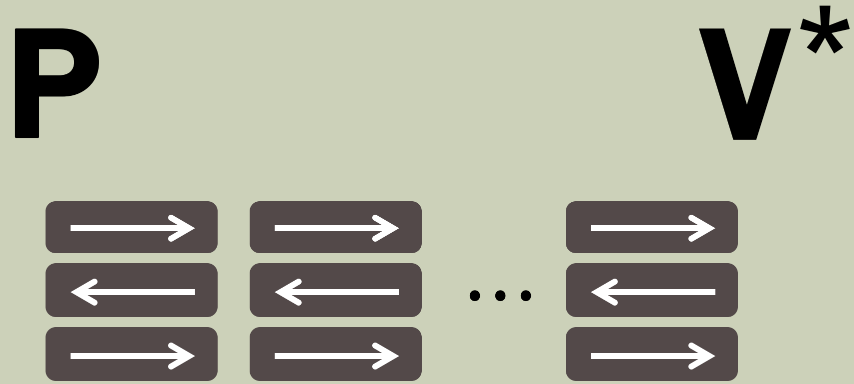
Public-coin: V's messages are contiguous chunks of its random tape (cannot use, e.g., hiding commitments)

Black-box simulator: uses V^*'s code as a black-box



- So far, all simulators were black box ($\exists S\ \forall V^*$ vs $\forall V^*\ \exists S$)
- Hard to envision how to use V^*'s code in any other way
- Reverse engineering is hard (later: code obfuscation)

Triviality of Black-Box ZK



<u>Triviality of BB</u> ZK: only $L \in \mathrm{BPP}$ have (negligible error)

- constant-round <u>public-coin</u> BB ZK proofs/arguments
- 3-round BB ZK proofs/arguments

- parallel repetition of HAM and QR_N protocols are public-coin
- applies to <u>any</u> constant number of rounds
- if $HAM, QR_N \notin BPP$, even private coins do not help for BB ZK

Triviality of const.-round public-coin BB ZK

Theorem [GK'91]: Suppose that L has a constant-round, negligible error, public-coin ZK proof. Then $L \in \mathrm{BPP}$

Proof idea:

- Consider a PPT BB simulator S
- Define a PPT V^* that on input $m_1, \ldots, m_{i-1}$ returns

$$m_i = f_k(m_1, \ldots, m_{i-1}),$$

where f_k is a pseudorandom function

- To decide if $x \in L$, run $S^{V^*}(x)$ and accept if and only if the resulting transcript is accepting

Pseudorandom Functions

<u>Definition</u>: $\{f_k\}$ is <u>pseudorandom</u> if f_k is not efficiently distinguishable from a random function R, given access to adaptively chosen $\left(x_i, f_k(x_i)\right)$

$$\mathbf{D} \underset{f_k(x_i)}{\overset{x_i}{\rightleftarrows}} f_k$$

<u>Candidate PRFs</u>:

- **AES:** $AES_k(x)$
- **GGM (any PRG):** $G_{x_n}\left(\ldots G_{x_2}\left(G_{x_1}(k)\right)\right)$
- **Degree t polynomial:** $a_0 + a_1 x + a_2 x^2 + \cdots + a_t x^t$
  (against $\leq t$ queries)

Triviality of const.-round public-coin BB ZK

Claim: If $x \in L$ then

$$Pr\left[S^{V^*}(x) = \text{ ACCEPT}\right] \geq 1 - neg(|x|)$$

Exercise: otherwise can distinguish the output of $S^{V^*}(x)$ from a real interaction $(P, V^*)(x)$

Claim: If $x \notin L$ then

$$Pr\left[S^{V^*}(x) = \text{ ACCEPT}\right] \leq neg(|x|)$$

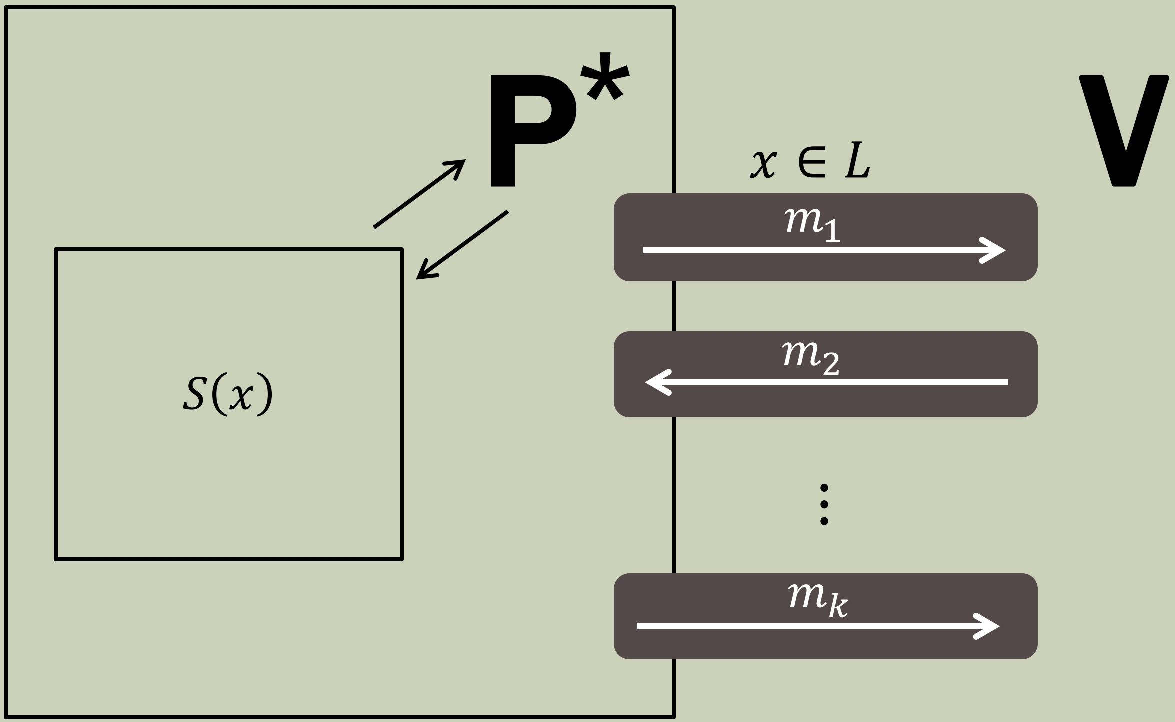
- Otherwise build a cheating prover P^*
- P^* convinces V that $x \in L$ with probability $1/poly(|x|)$

The Cheating prover

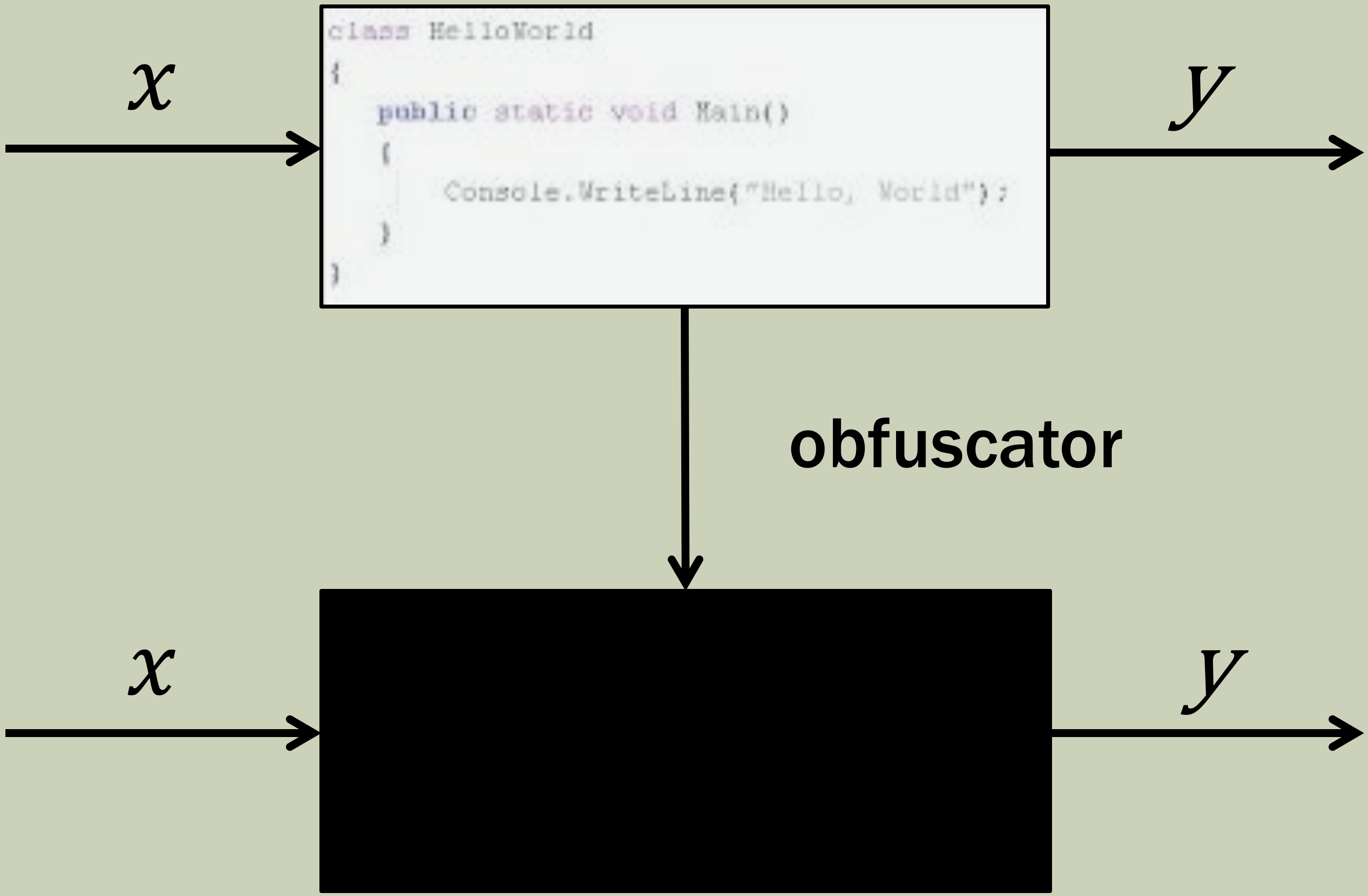
- P^* invokes S, answering S's queries as if he were V
- Occasionally (once for each round), P^* forwards the message to the real "outside" V
- P^* hopes that the message m_i that he chose to forward to the outside V is the one that will appear in S's output
- If P^* correctly guesses in all of the $k = O(1)$ rounds then he succeeds in making the outside V accept
- If the total number of queries made by S is t then

$$Pr[P^* \text{ correctly guesses in all } k \text{ rounds}] \geq 1/t^{O(k)}$$
$$= 1/poly(|x|)$$

The Cheating prover

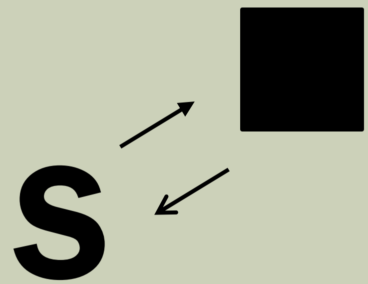


Program Obfuscation



Could be used to turn V^* into a black box

Obfuscation



- VBB obfuscation impossible in general
- In particular for "pseudo entropic" functions such as PRF
- [BP'12] – negative results for obfuscation can be turned into positive results for ZK

Parallel/concurrent Composition of ZK

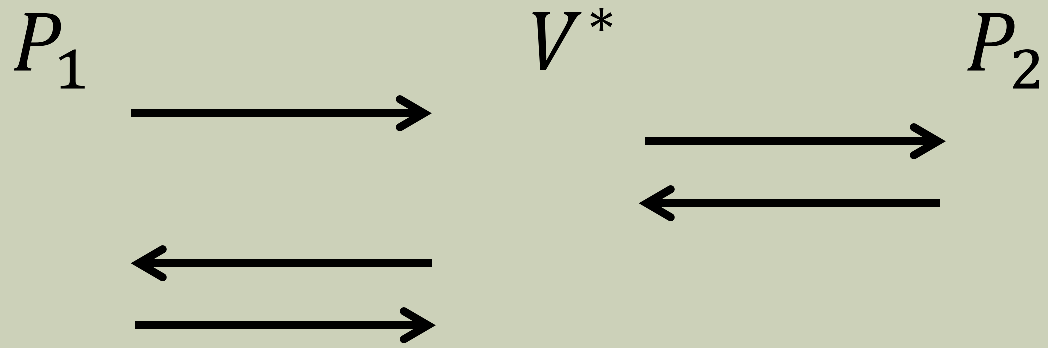
Failure of Parallel Composition of ZK

<u>Theorem</u> [F'90]: There exists a ZK protocol that does not retain its ZK properties when run twice in parallel

- There exist two provers P_1, P_2 such that each is ZK, but the prover that runs both in parallel yields knowledge
- Specifically, a cheating V^* can extract a solution for a problem that is not solvable in polynomial time
- P_1 sends "knowledge" if and only if V can solve a computationally hard challenge generated by P_1
- Solutions are pseudorandom but can be verified by P_1 (which is unbounded)
- P_2 solves such pseudorandom challenges

Failure of Parallel Composition of ZK

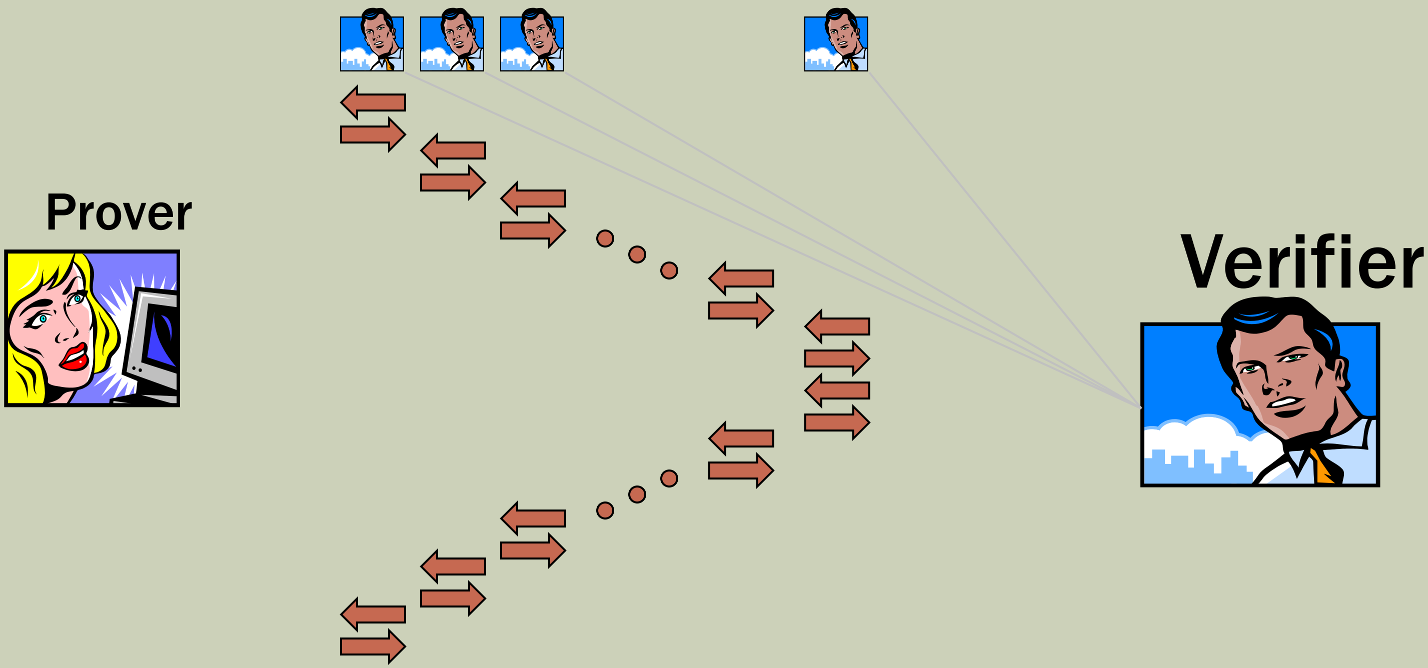
- Both P_1, P_2 are ZK
- P_1 because a $PPT\ V^*$ is unable to solve the challenge and so P_1 will not send "knowledge"
- P_2 because the solution cannot be verified in poly time



- Can be made to work for poly time P_1, P_2 using statistically-binding commitments and ZKPOKs

Concurrent Composition [F'90,DNS'97]

- No restrictions on synchronization of messages
- Adversary verifier determines the schedule
- Sequential and Parallel composition are special cases

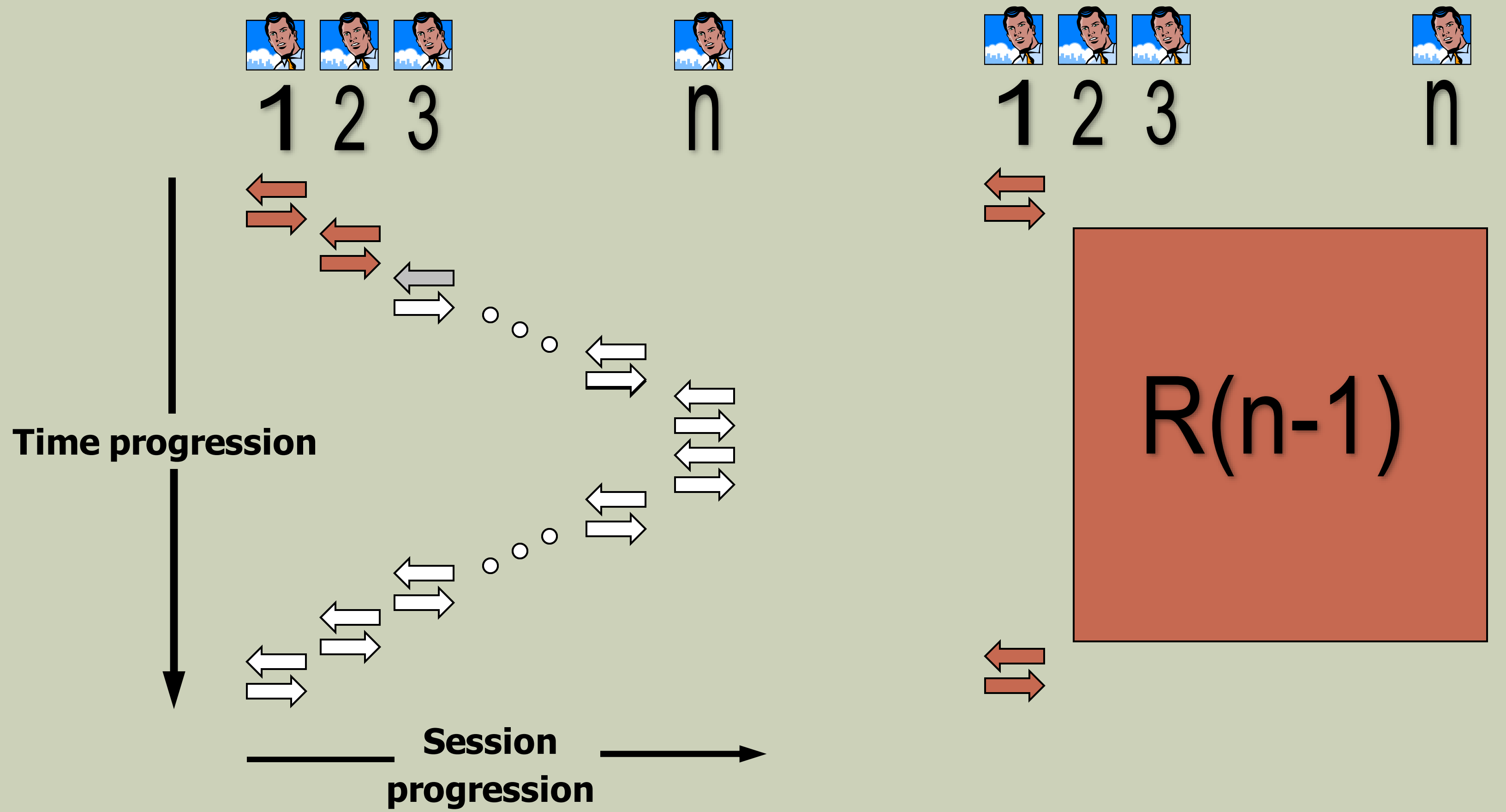


In the concurrent setting

- Should simulate polynomially many sessions.
- Simulator cannot proceed beyond end of a session without being able to convince verifier
- Thus, simulator must rewind every session
- Simulation work done for one session may be lost due to rewinding of other sessions

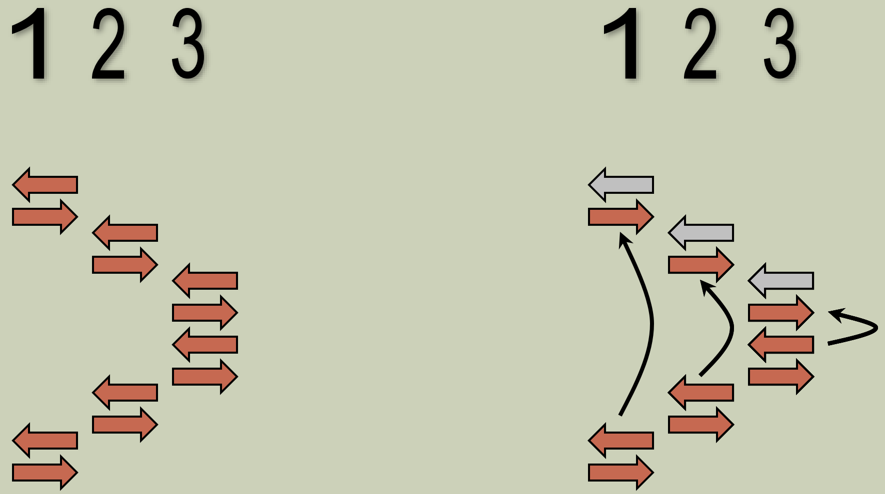
An Interleaved Scheduling [DNS]

4-message protocols are "hard" to simulate concurrently



Messages may depend on history of interaction

Why Simulation is Hard



$$W(n) = 2 \cdot W(n-1) = 2^{n-1}$$

The round-complexity of $c\mathrm{ZK}$

__Theorem__ [DNS'98]: **Every languages in NP has a constant-round concurrent ZK protocol in the "timing model"**

__Theorem__ [D'00]: **Every languages in NP has a constant-round concurrent ZK protocol with trusted setup**

__Theorem__ [KPR'98,CKPR'01]: **Only languages in BPP have BB concurrent ZK protocols with $o(\log n/\log \log n)$ rounds**

__Theorem__ [KP'01,PRS'02]: **Every languages in NP has a concurrent ZK protocol with $\omega(\log n)$ rounds**

Summary

Saw triviality ($L \in \mathrm{BPP}$) of:

- **Unidirectional/2-round ZK**
- **ZK with deterministic V, P**
- **Constant-round public-coin BB ZK**
- **failure of parallel composition**

Mentioned:

- **3-round BB ZK**
- **Difficulties in concurrent composition**

History

Hugo Krawczyk

Yair Oren

Joe Kilian

Cynthia Dwork

Ran Canetti

Erez Petrank

The End

Questions?